

Samstag, 28. November 2026, 15:58 Uhr
~8 Minuten Lesezeit

Das hybride Gespenst

Angebliche hybride und Cyberangriffe erschüttern Europa — und sind wahrscheinlich nicht das, als was sie uns verkauft werden.

von Felix Feistel
Bild: Collage mit Foto von Shutterstock.com (nblx, frank60)

Eine Welle hybrider Angriffe erschüttert Europa. Cyberangriffe und Drohnenvorfälle erfassen eine Reihe europäischer Staaten. Dahinter stecken angeblich die üblichen Verdächtigen: der böse Russe, die

hinterhältigen Iraner oder die höchst kriminellen Nordkoreaner. Tatsächlich weiß die Öffentlichkeit bei den meisten dieser angeblichen Vorfälle nicht einmal, ob sie tatsächlich stattgefunden haben. Und selbst wenn, bleibt unklar, ob tatsächlich derjenige dahintersteckt, den Behörden und Medien als Täter präsentieren. Diese angeblichen hybriden Angriffe könnten mehrere Zwecke erfüllen — vom Aufbau eines Feindbildes bis hin zum Great Reset.

Ein Gespenst geht um in Europa, das Gespenst der hybriden Angriffe und Cyberattacken. Das ist nun nichts wirklich Neues. In den vergangenen Jahren, insbesondere seit Beginn der heißen Phase des Krieges in der Ukraine, kam es immer wieder zu vermeintlichen oder tatsächlichen Cyberattacken und sogenannten hybriden Angriffen — was auch immer das genau heißen soll. Doch seit einigen Wochen erhöht sich die Schlagzahl — zumindest die der Schlagzeilen. Die aktuelle Phase der Bedrohungsinszenierung begann dabei vielleicht mit einer Reihe von Drohnenvorfällen. Davon war der für uns bedrohlichste wohl der sogenannte Drohnenvorfall am Flughafen Leipzig. Zur Erinnerung: Angeblich wurde zunächst eine Drohne gesichtet, die dann von einem Busfahrer aus der Luft geholt wurde — wie auch immer er das geschafft haben will. Diese Drohne soll Sprengstoff getragen und es auf die am Flughafen geparkten ukrainischen Militärfrachter abgesehen haben — was machen die eigentlich da?

Bei dem Sprengstoff, der hier angeblich zum Einsatz kam, soll es sich um **Semtex** (https://www.tagesanzeiger.ch/leipzig-was-der-sprengstoff-verraet-150588352539) gehandelt haben, einen Stoff, der in der Tschechoslowakei entwickelt wurde und bis heute in

Tschechien produziert wird. Obwohl also relativ wenig darauf hindeutet, dass es sich um eine russische Operation gehandelt haben könnte, machte die deutsche Bundesregierung Russland verantwortlich, warf dem Kreml hybride Operationen vor und machte dies zur Grundlage für weitere Sanktionen gegen das Land.

> ***Dem zum Feindstaat erklärten Russland wird hier also ein Vorfall angedichtet, bei dem im Grunde nichts passiert ist und von dem wir nicht einmal wissen, ob er tatsächlich stattgefunden hat.***

Letztlich müssen wir uns dabei auf Behördenangaben und Medienberichte verlassen. Und was davon zu halten ist, wissen wir spätestens seit der inszenierten Corona-Pandemie.

Dann folgte im Herbst eine Reihe von Cyberangriffen in der ganzen EU. In mehreren Ländern, darunter Frankreich, Belgien, Deutschland, Schweden und einigen anderen, waren Supermarktketten das Ziel. Dabei wurden Kühlanlagen umprogrammiert, sodass sie die Waren erwärmten, anstatt sie zu kühlen. Das führte zu teils massiven Schäden. Relativ bald darauf machten zuerst Frankreich und dann auch Belgien **den Iran** (https://orf.at/stories/3447996/) für diese Angriffe verantwortlich. Dabei gebe es Hinweise auf eine mögliche Beteiligung iranischer Akteure — so oder so ähnlich hieß es. Im Klartext: Nichts Genaues weiß man nicht, aber man kann ja schon einmal jemanden verantwortlich machen, der rein zufällig bereits Ziel eines imperialen Angriffskrieges aus der westlichen Hemisphäre ist. Dabei gilt im Bereich der Cyberangriffe eigentlich: Wenn alle Spuren auf den Iran — oder Russland — hindeuten, dann steckt ziemlich sicher nicht der Iran — oder Russland — dahinter. Denn erfahrene Hacker wissen ihre Herkunft zu verschleiern.

Weiter ging es mit einer Reihe von Bombendrohungen — erst gegen den europäischen Flugverkehr, dann **gegen Tausende Schulen**

(https://www.aljazeera.com/news/2026/11/12/more-than-1800-italian-schools-targeted-by-new-hoax-bomb-alerts) in Italien, Nordirland, Schottland und der Republik Irland **sowie später auch Deutschland** (https://www.swr.de/swraktuell/baden-wuerttemberg/bombendrohungen-schulen-100.html). Hinweise auf eine tatsächliche Bedrohung wurden dabei nicht gefunden. Verantwortliche Politiker wie Giorgia Meloni sahen darin **eher einen Cyberangriff** (https://www.tagesanzeiger.ch/bombendrohungen-6000-schulen-in-italien-evakuiert-245001154845) der dazu diente, Angst und Verunsicherung zu schüren. Denn die Drohungen gingen per E-Mail ein. Dabei gehörte nicht wirklich viel dazu. Die E-Mail-Adressen waren öffentlich einsehbar, das Maß an Koordination ist also überschaubar und legt einen Streich ebenso nahe wie einen gezielten Angriff eines feindlichen Akteurs. Einen Verantwortlichen will man noch nicht benennen, aber eines ist klar: Die Bedrohung ist real. Es kann alles und jeden treffen.

Auch die Kryptobörse Binance hat es getroffen. Diese wurde **Ziel eines Hackerangriffs** (https://en.wikipedia.org/wiki/2026_Binance_hack), bei dem 6,3 Milliarden US-Dollar an Kryptowährungen gestohlen wurden. Verantwortlich diesmal: nicht der Russe, nicht der Iraner, auch nicht der Chinese. Nein, es war der vierte im Bunde der Achse des absoluten Bösen: Nordkorea. Das ist immer der ultimative Trumpf der Bedrohung. Denn hier kann man Schuld zuweisen, ohne sich diplomatisch allzu sehr in Schwierigkeiten zu bringen. Von Nordkorea geht immerhin keine allzu große Bedrohung aus, zumindest nicht in Mitteleuropa.

Auch das angebliche Musterland der Neutralität und der Demokratie blieb nicht verschont. In der Schweiz wurden durch einen **Cyberangriff auf einen Softwarelieferanten für die Pensionskasse** (https://www.srf.ch/news/schweiz/cyberangriff-bundespensionskasse-publica-meldet-abgeflossene-daten) Daten der Versicherten abgegriffen. Dahinter soll **die Hackergruppe Akira**

stecken (https://www.srf.ch/news/schweiz/heikle-daten-gestohlen-hacker-fordern-loesegeld-nach-angriff-auf-publica-lieferantin), die Lösegeld für die Daten fordert. Die Gruppe wiederum ihre Wurzeln in — wer hätte es gedacht — **Russland beziehungsweise im russischsprachigen Raum** (https://cybelangel.com/blog/akira-ransomware-conti-successor-russian-threat-actor-profile/). Das sind zumindest die Einschätzungen verschiedener westlicher Geheimdienste. Auch hier also: Die Bedrohung kommt aus dem Osten. Und dieser Vorfall zeigt — und soll wohl auch zeigen — dass selbst neutrale Staaten wie die Schweiz betroffen sind.

Weiter ging es mit verschiedenen Angriffen auf die Behörden verschiedener Länder. In den USA war etwa das FBI betroffen, in Deutschland die BundID — eine Art prototypischer Digitaler ID, welche von der Bundesregierung angeboten wird um Verwaltungsangelegenheiten schneller und einfacher zu erledigen.

Damit ist niemand sicher vor einer Bedrohung aus den zu Feindstaaten erkorenen Ländern. Hier wird ein Bedrohungsszenario geschaffen, das im Herbst 2026 auf eine ganz neue Spitze getrieben wird. Und vielleicht ist genau dies das Ziel. Denn tatsächliche Beweise für all die Behauptungen gibt es eigentlich nicht. Wir wissen nicht, ob all diese Vorfälle überhaupt stattgefunden haben. Und selbst wenn, ist vollkommen unklar, wer dahintersteckt. Die Wahrscheinlichkeit, dass diese Vorfälle inszeniert werden, um eine Bedrohung durch äußere Feinde zu suggerieren, ist gar nicht mal so gering. Denn auf diese Weise könnten sich westliche Regierungen den **Rally-around-the-flag-Effekt** (https://www.manova.news/artikel/der-gemeinsame-grund) zunutze machen wollen, der besagt, dass sich die Menschen im Krisen- und Kriegsfall um ihre Regierung scharen.

> ***So wird ein Feind geschaffen, dessen Opfer der Westen ist und gegen den er sich zur Wehr setzen muss. Das***

> ***rechtfertigt jede Aufrüstung, jede verschärfte Rhetorik und sonstige Maßnahme — und letztlich auch den Waffengang.***

Denn wenn der Iraner, der Russe oder der Nordkoreaner in unsere Cybersysteme eindringen, unsere Lebensmittel vernichten, Vermögenswerte stehlen und Flughäfen angreifen, dann hilft letztlich nur noch, die Verantwortlichen von der Landkarte auszuradieren. Das ist zumindest die Logik, die auf diese Weise eine gewisse Berechtigung erhalten soll.

Denkbar ist aber auch ein anderer Hintergrund. Denn bereits seit Jahren macht das World Economic Forum (WEF) auf die Gefahren durch Cyberangriffe für das globale System aufmerksam — und das nicht ganz zu Unrecht. Denn die totale Vernetzung von allem — und zunehmend auch jedem — macht die globale Infrastruktur hochgradig anfällig. Ein flächendeckender Ausfall könnte schlagartig die ganze globale Ökonomie außer Gefecht setzen — mit katastrophalen Folgen. Daher üben die Verantwortlichen immer wieder in Planspielen mit dem Titel **„Cyber Polygon“** (https://www.weforum.org/projects/cyber-polygon) genau dieses Szenario. Und wie wir bemerkt haben, ist die Veranstaltung solcher Planspiele ein sicheres Zeichen dafür, dass diese Ereignisse früher oder später auch tatsächlich eintreten — Event 201 lässt grüßen.

Es ist also möglich, dass diese Vorfälle inszeniert werden. Hintergrund könnte auch hier die Idee des Great Reset sein. Bestandteil dieser Horrorvision ist die Einbettung aller Menschen in ein digitales Zwangssystem aus Digitaler ID, **zweckgebundener Digitaler Zentralbankwährung** (https://tkp.at/2024/02/12/deutsches-papier-digitaler-euro-zweckgebunden/), verbunden **mit einem Sozialkreditsystem** (https://tkp.at/2024/03/19/kanada-verknuepft-bankkonten-der-buerger-mit-sozialkreditsystem/), flächendeckender KI-Überwachung und extremer Online-Zensur. Dieses Zwangssystem

soll der vollkommenen Überwachung und Steuerung der Menschen dienen — was die Verantwortlichen auch **ganz offen so aussprechen** (https://tkp.at/2023/07/08/wef-digitales-geld-soll-buerger-vom-kauf-unerwuenschter-artikel-abhalten/).

Da man Menschen schlecht ihre Gewohnheiten abgewöhnen kann, sie den Nutzen Digitaler IDs vielleicht nicht so wirklich sehen und gerne am Bargeld festhalten würden, ist es also notwendig, sie auf andere Weise von der Notwendigkeit dieser Instrumente zu überzeugen. Die Lösung ist hier eine durch internationale Organisationen und staatliche Zusammenschlüsse kontrollierte digitale Struktur, die als sicher und wirksam angepriesen wird und an welche sich die Menschen spätestens dann freiwillig andocken werden, wenn das Finanzsystem kollabiert und erst über diese Struktur der Zugang zu Geld — und damit Waren — möglich sein wird. Natürlich wird all das nur zu unserer eigenen Sicherheit stattfinden und dient dem Schutz unserer Daten und Leben.

> ***Die Wahrheit könnte dabei aber vielmehr sein, dass genau jene Akteure, die sich schon die Corona-Pandemie ausgedacht haben, jetzt eine Cyberpandemie inszenieren. Denn genau mit dieser Bezeichnung hantierten die Verantwortlichen bei den vergangenen Planspielen.***

Dazu setzen sie das globale digitale System außer Gefecht, um es unter ihrer Kontrolle neu zu starten, die Menschen an die von ihnen geschaffene Infrastruktur anzudocken und damit die absolute Kontrolle über alle Daten und Konten zu erhalten. Auf diese Weise ist ein totalitäres System ungeahnten Ausmaßes möglich, das den Menschen ihr Verhalten bis ins Kleinste vorschreiben kann. Eine digitale Dystopie entsteht unter dem Vorwand ausländischer Cyberangriffe.

Dabei ist die Lehre, die man aus diesen angeblichen oder

tatsächlichen Attacken ziehen kann, eigentlich eine ganz andere. Vielmehr sollte man sich die Frage stellen, wie sinnvoll es wirklich ist, alles zu elektrifizieren und zu digitalisieren. Denn im Endeffekt wird das Leben der Menschen dadurch nur viel komplizierter und schwieriger, und — wie man sehen kann — viel angreifbarer. Eine viel einfachere Antwort, als die totalitäre Kontrolle einer globalen Digitaldiktatur wäre es, die Digitalisierung zurückzuschrauben, aus dem digitalen System zu einem großen Teil auszusteigen und nur wenige Berührungspunkte mit diesem zu haben.

Denn warum sind Kühltheken eigentlich mit dem Internet verbunden — über das sie dann angegriffen werden können? Warum muss jedes Gerät vernetzt werden, wenn man es auch viel effektiver analog steuern könnte? Denn jede digitale Vernetzung macht eine digitale Steuerung notwendig, die Spontaneität und Individualität gar nicht zulässt — weil sie nur bestimmte Parameter akzeptiert und bestimmte Verfahrensabläufe vorsieht. Zugleich wird, wie wir überall sehen können, die digital vernetzte Infrastruktur nur viel anfälliger — und daher unzuverlässiger. Schon jetzt befinden wir uns in einem digitalen Gefängnis, das noch dazu mit großen Unsicherheiten behaftet ist.

Eine digitale Diktatur, wie sie den Herrschenden derzeit vorschwebt, erhöht nur die Gefahren für den Einzelnen und für die Menschheit insgesamt. Und dafür braucht es keinen bösen Russen, Iraner oder Nordkoreaner. Es genügen die eigenen, heimischen Herrscher, die immer schon der größte Feind der Menschen waren — und das auch bleiben werden, wenn man sie lässt.



Felix Feistel, Jahrgang 1992, studierte Rechtswissenschaften mit dem Schwerpunkt Völker- und Europarecht. Schon während seines Studiums war er als Journalist tätig; seit seinem Staatsexamen arbeitet er hauptberuflich als freier Journalist und Autor. So schreibt er für manova.news, sowie auf seinem eigenen Telegram-Kanal. Eine Ausbildung zum Traumatherapeuten nach der Identitätsorientierten Psychotraumatheorie und -therapie (IoPT), erweiterte sein Verständnis von den Hintergründen der Geschehnisse auf der Welt. Von ihm erschienen bislang „**Corona – Next Level: Wie die nächste „Pandemie“ vorbereitet wird** (https://www.buchkomplizen.de/corona-next-level.html)“ im Hintergrund-Verlag sowie „**Sein und Bewusstsein – über die Grenze des Messbaren** (https://eticamedia.com/shop/produkt/bewusstsein/)“ bei Etica Media.